

Assessing Hazards from Explosives as Part of Explosives Facility Safety Cases

by S.M.Gilbert,

Systems and Facilities Engineering Division, Atomic Weapons Establishment (AWE),
Aldermaston, Reading, Berkshire, RG7 4PR, United Kingdom.¹

Abstract:

In many hazardous industries within the United Kingdom, there is a requirement for operators to produce a Safety Case for each of their facilities in order to demonstrate that their activities are carried out safely and without ill effect to persons' health or the environment.

A key aspect of the Safety Case is the risk assessment section, which identifies hazards and evaluates the control measures in place to determine the associated risks and demonstrate that these levels of risk are tolerable and kept as low as reasonably practicable. This paper presents a methodology for assessing condensed phase explosion hazards. The methodology has been developed in recognition of problems in risk assessment which are specific to processes and activities where explosive substances and articles are handled.

A fundamental difficulty is in the application of numerical data to estimate credible probabilities of initiation under accident conditions. Furthermore, it is often the case that organisational and human factors are critical aspects of hazard control in any given explosives facility. None of these aspects are readily quantifiable. Hence, there is little benefit in carrying out detailed probabilistic analysis when such great uncertainties in data exist. The approach advocated here places a strong emphasis on understanding the hazards and their controls, which is then demonstrated through rigorous evaluation based on strong qualitative arguments.

¹ Any views expressed are those of the author and do not necessarily represent those of the Department / HM Government.

| | | | | |
|---|------------------------------------|--|---|---|
| Report Documentation Page | | | <i>Form Approved OMB No. 0704-0188</i> | |
| <p>Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> | | | | |
| 1. REPORT DATE AUG 1996 | | 2. REPORT TYPE | | 3. DATES COVERED 00-00-1996 to 00-00-1996 |
| 4. TITLE AND SUBTITLE Assessing Hazards from Explosives as Part of Explosives Facility Safety Cases | | | | |
| 6. AUTHOR(S) | | 5a. CONTRACT NUMBER | | |
| | | 5b. GRANT NUMBER | | |
| | | 5c. PROGRAM ELEMENT NUMBER | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Atomic Weapons Establishment (AWE), Systems and Facilities Engineering Division, Aldermaston, Reading, Berkshire, RG7 4PR, United Kingdom, | | 5d. PROJECT NUMBER | | |
| | | 5e. TASK NUMBER | | |
| | | 5f. WORK UNIT NUMBER | | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | 8. PERFORMING ORGANIZATION REPORT NUMBER | | |
| | | 10. SPONSOR/MONITOR'S ACRONYM(S) | | |
| | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited | | | | |
| 13. SUPPLEMENTARY NOTES See also ADM000767. Proceedings of the Twenty-Seventh DoD Explosives Safety Seminar Held in Las Vegas, NV on 22-26 August 1996. | | | | |
| 14. ABSTRACT see report | | | | |
| 15. SUBJECT TERMS | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT Same as Report "SAR" | |
| a. REPORT unclassified | b. ABSTRACT unclassified | c. THIS PAGE unclassified | 18. NUMBER OF PAGES 21 | 19a. NAME OF RESPONSIBLE PERSON |

1.0 INTRODUCTION

This paper is produced in recognition of problems in risk assessment that are particular to processes and activities where explosive substances and articles are handled, i.e. materials belonging to UN Class 1.^[1]

The principal aims of carrying out Safety Case risk assessment on explosives facilities are to:

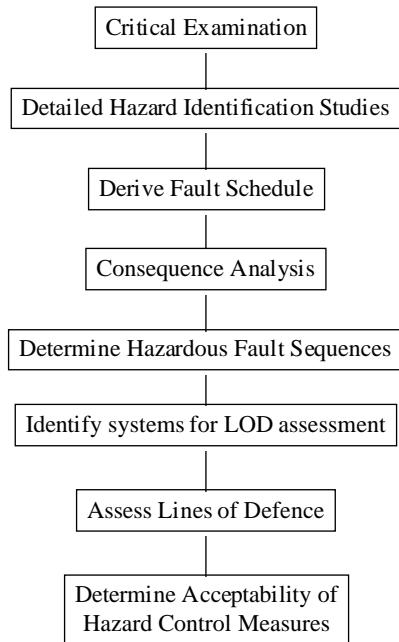
- # identify, in a systematic and comprehensive manner, the hazards and subsequent risks associated with the presence and operation of such facilities;
- # identify the controls in place to prevent or mitigate the harmful effects of the identified hazards (both engineered and procedural) - this serves to help identify safety related equipment and emphasise important elements of the safety management system;
- # enable the derivation of appropriate intervals of examination, inspection and maintenance for safety related equipment;
- # establish the limits and conditions of operation, i.e. define the ‘safe operating envelope’;
- # demonstrate the acceptability of continued operation, involving comparison with modern standards and risk acceptance criteria.

It is envisaged that organisational and human factors, e.g. access control, work procedures, will be shown to be critical aspects of hazard control on any given facility. As for initiation frequencies under accident conditions, these are not readily quantifiable. Hence, for explosives facility safety cases, there is little benefit in carrying out probabilistic risk analysis when such great uncertainties exist in data and when a rigorous assessment based on strong qualitative arguments will yield a better understanding of the hazards and their control.

It will be seen that much of the explosives risk assessment is carried out through deterministic (rather than probabilistic) analysis. Much of the deterministic analysis required draws on evidence of compliance with relevant modern standards. In the United Kingdom defence sector, to a large extent this function is served by the MOD (PE) Explosives Regulations^[2] (hereafter referred to as the *Explosives Regulations*). These indicate the systems which should be in place to prevent or mitigate hazards associated with explosives and are effectively specifications of appropriate defensive systems and procedures.

The framework for carrying out explosives risk assessment is illustrated in Figure 1.

Figure 1. Explosives Risk Assessment Methodology



1.1 *Applicability of the Methodology*

This methodology is applicable wherever explosive substances and articles of UN Class 1 are present. However, where radiological or toxic consequences are involved, the requirements for those particularly forms of hazard assessment will also need to be satisfied.

2.0 *HAZARD IDENTIFICATION*

Hazard identification is carried out through a combination of Critical Examination and detailed hazard identification techniques, which together should yield a comprehensive list of foreseeable hazards in the form of the fault schedule.

Crudely speaking, CE examines facility safety at the global system level, while detailed hazard identification studies are aimed at identifying specific fault conditions.

2.1 *Role of Critical Examination in Explosives Risk Assessment*

Critical Examination (CE) is a technical audit scheme which has been developed for the purpose of eliciting information and carrying out high level hazard analysis as a first step in facility Safety Case risk assessment. CE is applicable to all facilities irrespective of hazard type. Effective application relies on adequate preparation such that the study is directed and focused on the issues relevant to the facility. To help guide this process for explosives risk assessment, Annex A

suggests a number of explosives specific issues which ought to be considered within CE and detailed hazard identification studies.

An important preliminary task in preparing for explosives risk assessment is to establish the hazardous properties of the explosives in the states that they occur in the facility. It is particularly important to gather data concerning the sensitivity of explosives, from relevant sources such as Explosives Hazard Data Sheets, taking into consideration the influence of packaging, etc., and relating this to the normal process conditions. This activity is best initiated at the CE stage of risk assessment.

As well as identifying sources and gaps in information required specifically for risk assessment, through CE the assessors gain a general appreciation of the facility hazards and the strategies and arrangements in place by which they are controlled. Hence, from the outset, the necessary link is made between the risk assessment and the safety management system, as implemented at facility level. Evidence is sought regarding compliance with relevant legislation, codes of practice, modern standards, recognised industry best practice and company policies, principles, etc.. Particular emphasis is placed on examining the arrangements for carrying out risk assessment in the workplace, hence providing the basis for normal operations assessment and an indication of the extent of subsequent risk assessment required. For each area identified as requiring more detailed risk assessment, CE also enables the assessor to deduce the most appropriate means.

2.2 *Detailed Hazard Identification Studies*

Techniques such as HAZOP and FMEA may be applied to examine hazardous activities in detail to identify the hazards that may arise through deviating from safe operating conditions. Issues such as potential sources and mechanisms of ignition or initiation are most appropriately identified by detailed studies of each specific activity under consideration.

It should be noted that many of the more 'safety' critical aspects of explosives facility operations are those requiring human intervention, often involving short sequences of simple manual tasks. For these, some form of human error identification based on task analysis may be necessary to adequately identify potential accident sequences.

Hence, combined with the output of CE, the schedule of hazards identified should be as comprehensive as possible, irrespective of the particular technique applied, whether it be HAZOP, FMEA, human error analysis or any other method. This is achieved through production of the fault schedule, which serves as the definitive list of faults to be assessed. For explosives facilities, the safeguards and mitigating factors would be expected to include those specified in the *Explosives Regulations*.

It is stressed that explosives hazard identification should not be done in isolation - the above are merely special considerations to be applied in addition to identifying other types of hazard arising from a facility's activities.

3.0 CONSEQUENCE ANALYSIS

By the very nature of explosives, the effects of accidental ignition / initiation are largely immediate and entail severe consequences. The magnitude of effects is largely determined by the quantity of explosive material involved - the type of effects is largely determined by the hazard division.

In addition to acute effects, many explosive substances possess toxic properties which may lead to chronic effects on the health of workers coming into contact with these materials. The potential impact of toxic effects should also be assessed as one of the hazards from normal operations (see Section 5.1).

Section 3.1 presents the background information behind the approach taken to consequence analysis and Section 3.2 builds on this to summarise how the method should be applied.

3.1 *Background to Consequence Analysis Method*

3.1.1 Hazards Presented by Explosions to Persons in the Immediate Vicinity

This section describes the approach for establishing the potential consequences to persons in the immediate vicinity of an explosion.

As a guide, the level of harm that may result from accidental initiation may be related to the mass of explosive involved. Some indication of the potential to harm is given by considering the effects of explosions of small quantities of high explosives inside a small single storey (6m x 6m) building [Ref. 3]:-

1g of explosive:

- any person holding the explosive could receive serious injury

10g of explosive:

- any person close to this quantity of explosive at the time of initiation would receive very serious injuries
- 1% of persons at a distance of 1.5 metres away are liable to eardrum rupture

100g of explosive:

- 1% incidence of eardrum rupture at 3.5 m
- 50% incidence of eardrum rupture at 1.5 m
- persons in very close proximity to explosion, e.g. holding the explosive, almost certainly killed.

500g of explosive:

- complete structural collapse of brick-built building is most likely
- steel or concrete framed building would probably survive
- persons very close to explosion almost certainly killed

- persons close to explosion will be seriously injured by lung damage, fragmentation effects and bodily displacement
- almost all persons within the room will sustain perforated eardrums.

For quantities in excess of half a kilogram, it may be assumed that personnel within the room will not survive.

Hence, a rough correlation may be made between the quantity of explosives involved and the level of harm (according to the consequence categories presented in Annex B). For small quantities of explosive, it is useful to distinguish between persons working with the explosive at the time of initiation and those not directly involved, but elsewhere in the room. Operating procedures and license conditions serve to limit the number of personnel exposed to explosion hazards.

Table 1. Inventory-Based Accident Severity Categories

| Quantity of explosives (g) | Personnel Explosives | Handling | Personnel elsewhere in room/building |
|----------------------------|-------------------------|----------|---|
| < 1 | Serious | | No injury |
| 1 - 10 | Serious | | Minor |
| 10 - 100 | Critical | | Important |
| 100 - 500 | Critical | | Serious |
| > 500 ^(a) | Critical | | Critical |

(a) If two or more people are in the room/building at the time, they are all likely to be killed by the explosion. The accident severity would then become 'Catastrophic'. Hence, in allocating an accident severity category it is necessary to consider prescribed safe manning levels.

(b) Note that for each range, the accident severity category is based on the effects at the upper limit. This banding is therefore considered to be generally pessimistic.

(c) Fragmentation (shrapnel) effects should also be considered in assigning the accident severity category.

If persons are likely to be located in some other part of the building at the time of explosion, the assessment should demonstrate adequate separation from the effects. For example, for incidents arising from machining operations, the deterministic analysis should demonstrate that the control room is adequately designed to withstand the explosion effects, including blast and fragment attack, along with a demonstration that adequate access control prevents occupation of restricted areas during such operations.

3.1.2 Hazard Presented by Explosions Inside Buildings to Persons Not Under Cover but Within the Explosives Area

At any given time, there are likely to be personnel within the explosives area but not within buildings, i.e. moving between buildings, maintaining building exteriors, grass cutting, etc.. Such

personnel may be more exposed to the direct effects of an explosion than those in the shelter of purpose-built explosives buildings. Access control measures should aim to keep the number of personnel working within the explosives area to a minimum and temporarily prevent access to areas where explosives operations are being carried out, e.g. during explosives machining.

3.1.3 Explosions Occurring in the Open

For the purposes of movement (in the open within designated explosives areas or along site roads) or transport (along public roads), it is necessary to take explosives from buildings and thereby remove a significant layer of containment. Little or no credit may be taken for blast mitigation, either by the explosive container or the vehicle load compartment - indeed, these may serve to provide an additional source of high energy fragments. Much greater emphasis is placed on preventing the event through safeguards, both engineered (e.g. packaging and vehicle construction) and managerial (e.g. approved consignments, driver training and competence).

Bearing in mind these considerations, it is suggested that an appropriate approach is to assume pessimistic consequences for persons in the vicinity at the time of the explosion and to concentrate on examining the likelihood of occurrence. The scenario becomes important in defining those at risk, since incidents of explosions in transit may or may not be preceded by some precursor event (e.g. engulfing fire), which takes time to develop (15-20 minutes, say). This delay could provide time for evacuation (or conversely time to attract others to the scene) before initiation occurs.

More detailed consequence analysis^[4,5] would only then be warranted if the risk (based on conservative assumptions regarding consequences) appears unacceptable.

3.1.4 Hazard Presented by Explosions Inside Buildings to Populations Under Shelter or External to the Explosives Area

At AWE premises and Ministry of Defence establishments, a regime of licensing is in place to prescribe the operations and limit the quantities of explosive material permitted in a given explosives complex/building/room. The license conditions for AWE premises are set by the Chief Inspector of Explosives MOD (PE), using the guidance presented in Quantity-Distance (Q-D) tables issued by the Explosives Storage and Transport Committee (ESTC) as the basis for determining quantity limits. These refer to the relationship between a quantity of explosives and the distance necessary to sufficiently limit the severity of the effects of the accidental functioning of the explosives and to adequately protect the exposed site under consideration.

The Q-Ds have been derived empirically from a considerable amount of incident data, much of which was collected during the earlier years of explosives manufacture when the rate of occurrence of accidents was much more frequent than today. This has subsequently been backed up by numerous trials programmes specifically aimed at validating the criteria further.

It is stressed that the Q-Ds do not assure safety. It is impracticable to prescribe distances which would guarantee absolute immunity from the risks of propagation, damage or injury. In deriving the Q-Ds, the ESTC adopted the premise that no matter how good the preventive measures which can and should be enforced, sooner or later an accidental explosion may occur. The Q-D concept is taken to represent an acceptable compromise between absolute safety and reasonably practicable considerations of risk limitation.

Clearly, in assessing the extent of hazards beyond the immediate confines of an explosives building, adherence to Q-Ds is a principal consideration in any safety justification argument. Hence, the prime consideration in the (deterministic) analysis of the extent of explosion consequences is that a valid license has been granted by the relevant authority, taking into consideration the guidance presented in the Q-D tables. This should be tempered by an assessment of the design features which contain or direct explosion effects at source (blast and missiles), together with the level of shelter afforded in potentially affected areas.

Table 2 defines the situations where the consequence may legitimately be claimed as being bound by license conditions.

Table 2. Situations Where Protection is Afforded by the Q-D Licensing System.

| Afforded | Not Afforded |
|---|----------------------------------|
| Public and workers sheltered in buildings (Exposed Sites) while work is in progress | Potential Explosion Site workers |
| | Unsheltered workers |
| | Work in transit |

3.2 Method for Assessing Consequences of an Explosion

This section builds on the background information presented above to summarise how the method should be applied. For each accident scenario considered, the approach is broadly as follows:

1. Define the explosive involved.

- hazard division (defines types of effects)
- mass of explosive involved (defines magnitude of effects)

2. Identify populations at risk and location relative to explosion site.

- location of explosion
- location of persons at time of ignition / initiation (defines approach)

3. Establish the effects on persons exposed.

- mitigating features
- separation distance

Hence, the analysis should consider the influence (or absence) of explosion mitigation features (inherent structural properties, blast protection/ containment, etc.) as well as the potential consequence implications of unauthorised access to exclusion areas. Table 2 defines the situations where compliance with Q-D criteria may be legitimately claimed as a mitigating factor.

The following subsections define the approach to be taken for broad scenario types, largely based on events involving HD 1.1. For events involving explosives of other hazard divisions this approach might lead to pessimistic outcomes where it might be more appropriate to address a specific effect, e.g. the thermal hazard from HD 1.3 explosives. A note discussing an approach for dealing with HD1.4 explosives is included as Section 3.3.

3.2.1 Assessing the Consequences of Explosions on Persons in the Immediate Vicinity

Accident severity should be determined according to the scheme presented in Table 1.

3.2.2 Assessing the Consequences of Explosions Inside Buildings on Persons Not Under Cover but Within the Explosives Area

Since Q-Ds only serve to mitigate the consequences as far as they affect other buildings and locations accessible to the public, compliance with Q-D based license conditions can not be claimed as a Line of Defence. Instead, consequences are mitigated against by excluding personnel from defined cover areas set up over the duration of specific hazardous operations. The efficacy of the exclusion distance and access control measures need to be assessed in order to determine the risk to these groups of people.

3.2.3 Assessing the Consequences of Explosions Occurring in the Open

For persons in close proximity, accident severity may be determined according to the scheme presented in Table 1.

For other exposed populations, the approach is in the first instance to assume pessimistic consequences for persons in the vicinity at the time of the explosion. More detailed consequence analysis^[4,5] would only then be warranted if the risk (based on conservative assumptions regarding consequences) appears unacceptable.

3.2.4 Assessing the Consequences of Explosions Inside Buildings on Populations External to the Explosives Area

Essentially, compliance with the relevant Q-Ds constitutes an extra Line of Defence in protecting persons ex-facility in addition to those already acting to prevent an explosion occurring in the first place. In effect, this should compensate for the additional duty of care owed to the public

(and personnel ex-facility) which is reflected in the more stringent risk tolerability criteria afforded these groups.

3.3 Note on Assessing the Hazard from HD 1.4 Explosives

Articles of minor ordnance are typical of the explosives which fall into HD 1.4. Packages of Compatibility Group S are the simplest case in that potential hazardous effects are wholly contained within the package (see footnote to Section 1.1). Where other compatibility groups are concerned, any effects are largely confined to the package and no projection of fragments of appreciable size or range is to be expected.

Provided the article is in its properly packaged state risks from HD 1.4 explosives may effectively be screened out on consequence alone. If the container's integrity is compromised, by fire for example, or the explosive is out of its container then hazardous properties of the article need to be specifically addressed.

Although these articles are unlikely to present any significant explosion hazard, there may be other hazardous properties to consider, e.g. toxic fumes may be given off in a fire, etc..

4.0 LINES OF DEFENCE ASSESSMENT

Much dependence is placed on human actions and management systems to control explosives hazards. As such, a strong qualitative approach is likely to yield the most suitable demonstration that explosives hazards are adequately controlled. For explosives risk assessment, this is achieved by conducting deterministic analysis which is presented in the form of a Lines of Defence assessment. It entails a reasonably detailed examination of engineered features and managerial controls and a robust justification for assigning Line of Defence (LOD) status to the safety systems in place.

The preferred approach is to combine fault tree analysis with the Lines of Defence analysis. Apart from extremely simple fault sequences (where LOD assessment may be applied directly) fault trees should be used to represent qualitatively all fault sequences which could give rise to specified top events, e.g. death or serious injury to operator from an explosion. The analysis needs to consider all explosives-related activities on a facility. This is achieved by ensuring that all fault sequences identified in the fault schedule are represented in the fault trees.

If warranted the deterministic analysis may be supported by more detailed studies of some of the more safety critical aspects of the facility's operation. By nature of the activities carried out on explosives facilities, these would probably take the form of detailed human factors studies.

Section 4.1 presents the background information behind the approach taken to Lines of Defence analysis and Section 4.2 builds on this to summarise how the method should be applied.

4.1 *Background to Lines of Defence Analysis*

4.1.1 Fault Tree Analysis

The fault tree serves both as an illustration of how the incident may be brought about and (if used to its full potential) as an analytical tool in deriving the minimum cut sets. The lines of defence against the faults contained in these cut sets may then be identified and assessed in terms of their effectiveness in preventing the top event from occurring.

Furthermore, the use of fault trees is beneficial since it portrays defence in depth, one of the principal philosophies in underpinning explosives safety. Used in conjunction with the deterministic analysis, the fault tree structure demonstrates whether LODs are properly deployed against all threats and where ‘weak links’ may exist.

4.1.2 Deterministic Analysis of Safety Systems Against Fault Sequences

Having established the structure of the fault trees, it is necessary to relate the safety systems (safeguards and mitigating factors) to the identified cut sets or subevents.

The assessment is carried out by determining whether the associated safety measures [systems] comprise one or more Lines of Defence against the fault using the Lines of Defence qualification criteria. The process involves consideration of all characteristics affecting the performance of the system(s). Namely, the challenges placed on the system [demand], the required safety function of the system [design basis] and its continuing ability to deliver the required function upon demand [capability]. The determination must be made in context, i.e. with respect to each specific fault sequence.

Potential consequences have a bearing on the deterministic assessment in that they must be compared with the design basis of safety systems, for example, to ensure that the effects of an explosion are contained or otherwise protected against. Safety measures such as blast protection and containment systems must be shown to be commensurate with the potential explosion effects.

Robust arguments are required in justifying whether safety measures qualify as Lines of Defence. To qualify as a LOD, it must be shown that a safeguard (or combination of safeguards) provides adequate protection in preventing the event (or subevent) under consideration from occurring. It is emphasised that the safeguards must be assessed specifically in terms of the fault they are intended to prevent. For instance, where credit is to be claimed for ‘training’ or ‘procedures’, the deterministic assessment should consider those specific aspects that assist in preventing occurrence of the fault or mitigating against the consequences.

Evidence of safeguards’ collective ability to qualify as a LOD should be based around considerations with respect to the following criteria:

Table 3. ‘Line of Defence’ Qualification Criteria

| |
|--|
| # a substantial capability margin over the maximum perceivable demand, through conservatisms in design which makes large allowances for uncertainty; |
| # regular and appropriate inspection, test and maintenance (or audit of managerial controls); |
| # robustness against human error and incorrect actions; |
| # capability to provide the minimum required functional output with any single active component failure, i.e. redundancy; and |
| # quality assured design, manufacture and installation (or implementation of managerial controls). |

The evidence required to support various assertions will largely be anecdotal. However, where numerical data directly applicable to the operation under consideration are available, they may be employed to strengthen the basis of the assessment. That is to say, well documented operational experience may be referred to and utilised to back up the qualitative Lines of Defence assessment. With specific regard to initiating event frequencies, again operational experience may be used if it helps demonstrate the demand likely to be placed on a given system, e.g. lightning strike rates for a given area. Hence the periodicity of maintenance, inspection, checks, etc. required to maintain a system’s capability (e.g. lightning conductors) may be determined (though for many safety systems these periods are prescribed through various regulations and recognised standards and a demonstration of compliance may be all that is required - where these are supplemented by local procedures, these again should be utilised to strengthen the arguments).

Assessing the adequacy of safeguards and mitigating factors is key to the Lines of Defence assessment. Merely listing the systems against the fault is not enough to satisfy the requirements of the (deterministic) risk assessment and is therefore not acceptable.

As a guide to risk assessors more familiar with probabilistic risk analysis, a cautious comparison may be made with numerical criteria. It is tentatively suggested that to qualify as a LOD, an event against which the safeguards are intended to protect should occur at a frequency no greater than 10^{-3} per year.

4.1.3 Risk Acceptability Criteria

Adopting the above definition of a LOD, at least one LOD is required (with ALARP argument) to justify continued operation. Two or more independent LODs provides confidence that risks are broadly acceptable. For complex systems, the independence of LODs may be readily confirmed by the minimum cut sets approach.

Credit should also be claimed in the LOD analysis for any other safeguards whose effect is to prevent a given event but would not meet the requirements of a LOD, e.g. general provisions and safeguards against other faults which indirectly contribute to preventing the fault under consideration.

4.2 Method for Assessing Lines of Defence for Explosives Risk Assessment

4.2.1 Generating Fault Trees

All ‘assessed faults’ identified in the fault schedule should be represented in the fault trees (unless the faults are so straight forward to warrant direct LOD assessment).

Top events should specify the level of injury and the persons at risk, e.g. death or serious injury to operator.

In addition to safeguards against direct and subsidiary causes of ignition / initiation, the fault tree needs to allow a representation of where other important safety factors fit in, e.g. access control measures, safety assurance through characterisation, etc..

Fault trees must be developed to a sufficient level of detail to enable a meaningful LOD assessment to be carried out. Having established the correct fault tree structure, candidate subevents and base events should be identified as subjects for the subsequent LOD analysis. This is most effectively achieved through the derivation of minimum cut sets.

4.2.2 Assigning LOD Status to Safety Systems

As detailed in Section 4.1.2, systems should be assessed deterministically to demonstrate capability in defending against the specific fault sequences being considered. The objective should be to demonstrate that the safety significant systems, as claimed within the safety case, can provide the safety function required of them.

In applying LOD assessment the twin concepts of ‘conservative proof of capability’ and ‘tolerance of any single credible failure’ should be kept in mind. For example, inherent properties of the explosive should be considered in respect to failure tolerance, taking into account any demonstrable safety margin between perceived magnitude of insults and known characteristics. Where such judgements cannot be made convincingly then LOD status should be denied until better evidence to support the qualification is made available.

The results of an explosives LOD assessment should feature the following:

- a sufficiently detailed description of the safety systems (whether engineered or managerial) and their intended action against a fault;
- measures required to maintain the capability of the safety systems;
- robust justification for assigning LOD status against the qualification criteria; and
- assessment of collective performance of LODs against fault propagation to top event.

The final point entails not just a count of LODs but also some consideration of independence and deployment within the fault tree structure. Hence, it ought to be possible to demonstrate defence in depth and to identify key safety systems and potential ‘weak links’ in the system.

4.2.3 Assessing Whether Risks are Acceptable

For top events involving death or serious injury to explosives workers, one LOD is required (with ALARP argument) to justify continued operation. Two or more independent LODs provides confidence that risks are broadly acceptable.

Additional protection afforded the public and other persons ‘ex-facility’ should be provided through compliance with the Q-D based licensing conditions, which essentially comprises an additional LOD. Situations where this LOD may legitimately be claimed are defined in Table 2.

An ALARP argument should entail identification of possible risk reduction measures and a discussion of the perceived benefit in terms of risk reduction versus the cost of implementation. Factors such as the remaining lifetime of the facility, ease of implementation, practicality and potential interference with work activities should be provided as the basis for deciding whether to adopt or reject a change to the system.

5.0 RESULTS OF THE RISK ASSESSMENT

Results from the risk assessment should demonstrate:

- all reasonably foreseeable forms of explosives hazard have been identified;
- fitness for purpose of safety systems, i.e. design intent and measures to assure continued capability; and
- defence in depth, identifying key defences and any potential areas of weakness.

The results and conclusions of the risk assessment should be tempered with operational experience and incident data wherever such information is available.

The remainder of this section deals with hazards arising from normal operations and provides guidance on the deductions that can be made from the risk assessment.

5.1 Hazards Arising from Normal Operations

The assessment of risks during normal operations should be almost entirely based on the deductions from Critical Examination (CE), complemented with more detailed analysis of incident and health records.

Control of exposure to toxic effects of explosive substances should be treated as for any other substance hazardous to health, i.e. by assessing adequacy of Coshh^[6] assessments, specific control measures, etc..

5.2 Fault and Accident Conditions

Due to the severity of consequences, assessment of risks to explosives workers is predominately dependent on the LOD assessment. Therefore the demonstration of acceptability will rely heavily on the arguments presented in that section. It must be shown that sufficient controls are in place to keep the risk of such an event tolerable and as low as reasonably practicable. To achieve this it will be necessary to make a rigorous comparison with appropriate modern standards.

5.3 Sensitivity Analysis

Where uncertainties exist in the assessment of the most ‘safety’ critical aspects, more detailed analysis may be required to confirm the findings. The risk assessor should examine the basis and influence of key assumptions made in the assessment. On the ‘frequency’ side, this could take the form of detailed human factors work. On the ‘consequence’ side, more detailed modelling of the explosion effects may be required.

The results and conclusions of the risk assessment should be tempered with operational experience wherever such information is available.

5.4 Identification of Safety Systems

The risk assessment should enable the identification of safety systems and their status, according to the classification scheme adopted. In addition, the deterministic assessment should have established the regime of inspection, testing, etc. required to maintain the capability of engineered safety systems and hence enable the examination, maintenance, inspection and test (EMIT) schedule to be derived.

5.5 Safe Operating Envelope

In terms of explosives operations within buildings, the consequences of an event are bounded by the license limits set by the competent authority. These specify limits such as explosives quantities and manning levels.

Limiting values for parameters aimed at preventing occurrence of an inadvertent explosion should be established from the deterministic analysis. These include maximum machine feed rates, safe working loads on vehicles and lifting equipment, stacking limits, maximum heights of lift, storage, etc..

Requisite safe operating conditions should also be specified, outside of which operations would not be permitted. Examples would include rules governing the physical location of explosives to be segregated in storage, or conditions to be satisfied before work activities may proceed.

6.0 CONCLUSION

Broadly speaking, the hazard control philosophy for explosives facilities is to avoid situations which could give rise to accidental initiation while conceding that an explosion might in any case still occur and hence provide protection through strong mitigating factors, mainly through containment of explosion effects and Q-Ds.

By concentrating on protecting the explosives worker through ensuring that the frequency of initiating events is kept as low as reasonably practicable, the risks to all others is automatically reduced. Greater protection afforded to public and others 'ex-facility' is effected via Q-Ds.

Hence, the requirements for explosives risk assessment are to:

1. Adopting the inherently conservative approach to assessing consequences, examine the adequacy of hazard control measures in preventing ignition / initiation when persons may be exposed, and
2. Demonstrate through deterministic analysis that adequate protection is afforded to persons outside the immediate confines of an explosives complex/building/room.

Essentially, where consequences are rated as 'Serious' or above, continued operation may only be justified if the risk assessment demonstrates that at least one LOD exists for each explosives operation carried out on the facility. This must be backed up with a robust ALARP argument, unless confidence is provided in the form of two or more independent LODs.

The ALARP argument should consider possible risk reduction measures and then recommend implementation or give justified reasons against.

7.0 REFERENCES

- [1] UNITED NATIONS - Committee of Experts on the Transport of Dangerous Goods. (1995). Recommendations on the Transport of Dangerous Goods {aka the 'Orange Book'}, 9th Revised Edition. (New York: United Nations) ST/SG/AC.10/1/Rev.9.
- [2] MOD (PE) Explosives Regulations (1986), as amended.
- [3] MERRIFIELD,R. (1991). Safe Handling Requirements During Explosive, Propellant and Pyrotechnic Manufacture. Health and Safety Executive, Specialist Inspector Reports, No.31.
- [4] GILBERT, S.M. (1994). A Model for the Effects of a Condensed Phase Explosion in a Built-Up Area. PhD thesis (Loughborough University of Technology).

[5] GILBERT, S.M, LEES, F.P and SCILLY,N.F. (1994). A Model for Hazard Assessment of the Explosion of an Explosives Vehicle in a Built-Up Area. Department of Defense Explosives Safety Seminar, Miami, August 1994.

[6] The Control of Substances Hazardous to Health (COSHH) Regulations, 1994.

8.0 ACKNOWLEDGEMENT

The author would like to express his thanks to numerous colleagues within AWE for providing their valuable insight and comments during the development of the methodology presented in this paper.

© British Crown Copyright 1996 / MOD

Published with the permission of the controller of Her Britannic Majesty's Stationery Office.

Annex A Explosives Specific Hazard Control Issues

Although it is not exhaustive, the following is a list of explosives specific issues which ought to be addressed within the risk assessment and examined as part of the CE and detailed hazard identification stage.

SENSITISATION

- Segregation
 - chemical compatibility
 - explosives compatibility (mixed inventories)
 - material, e.g. contamination from grit, rust
- Ageing (chemical degradation / decomposition)
- Ambient conditions (temperature, humidity)

IGNITION / INITIATION

The following is a list of direct (physical) causes and subsidiary causes of ignition or initiation. All should be considered during hazard identification studies, leaving any relationships between each type to be established by subsequent analysis.

- Electricity
 - Static
 - charge by separation
 - induction
 - friction/ contact
 - earthing/ discharge/ spark
 - Dynamic
 - Lightning
- Radiation
 - X-Ray
 - EMR
 - Radioactivity
 - Shielding
 - Radio frequencies
- Mechanical
 - Impact
 - collision
 - tools
 - falling objects
 - flying objects (missiles)
 - shock (air/ ground)
 - Friction
 - crushing
 - dragging/ sliding
 - stress/ shear, e.g. stacking too high

- Thermal
 - Spigot
 - Fire
 - Overheating
 - machinery fault
 - maloperation
 - Hot surfaces
 - Hot work
 - Extreme temperature
- Chemical reaction
 - Contact with incompatible chemicals / materials
- Software faults
 - CNC programming errors
 - Control & instrumentation faults
 - Erroneous input/output with operator
- Human error
 - Operator
 - Maintainer
 - Organisational factors
- External events
 - Other facilities/ sites
 - accident escalation
 - imported hazards, e.g. incorrect deliveries
 - Services/ utilities (gas, power lines, etc.)
 - Transport (aircraft, road, rail)
 - Severe weather
 - Seismic
 - Malicious intent (grievances, terrorism)

SAFEGUARDS / MITIGATION

The following safety assurance measures should be examined to establish their adequacy and robustness in preventing or mitigating against explosion effects. Potential means by which these systems might fail should be examined as part of the CE and hazard identification process.

- Characterisation (demonstration of explosive's resistance to insults)
- Packaging (certification for handling specified explosive articles/substances)
 - Thermal insulation
 - Electrical insulation
 - Impact/ shock resistance

- Access control
 - Contraband
 - Barriers
 - Remote operations
 - Interlocks
- Separation (other explosives, people, domino effects)
 - Distance, e.g. Q-Ds and licensing limits (max. HE mass)
 - Containment
- Contingency
 - Emergency response
 - Passive protection, e.g. fuses
 - Active protection, e.g. sprinklers/deluge
- Competence assurance
 - Training
 - Culture
- Systems of Work
 - Standard procedures, work instructions, operating rules, etc.
 - PTW

ANNEX B

Table B1. Accident Severity Categories

| Category | Explosives Workers | Others On Site & Public |
|--------------|--|---------------------------------|
| Catastrophic | Multiple deaths | Single death |
| Critical | Single death | Non-fatal injury |
| Serious | Serious injury or occupational illness, causing lasting impairment. | Restrictions, e.g. road closure |
| Important | Injury lasting more than 3 days (reportable under RIDDOR) ^(a) | N/A ^(b) |
| Minor | Injury lasting less than 3 days (non-reportable under RIDDOR) ^(a) | N/A ^(b) |

(a) Reporting of Injuries, Diseases and Dangerous Occurrences Regulations.

(b) Any incident having an impact outside the facility boundary is considered to be serious.